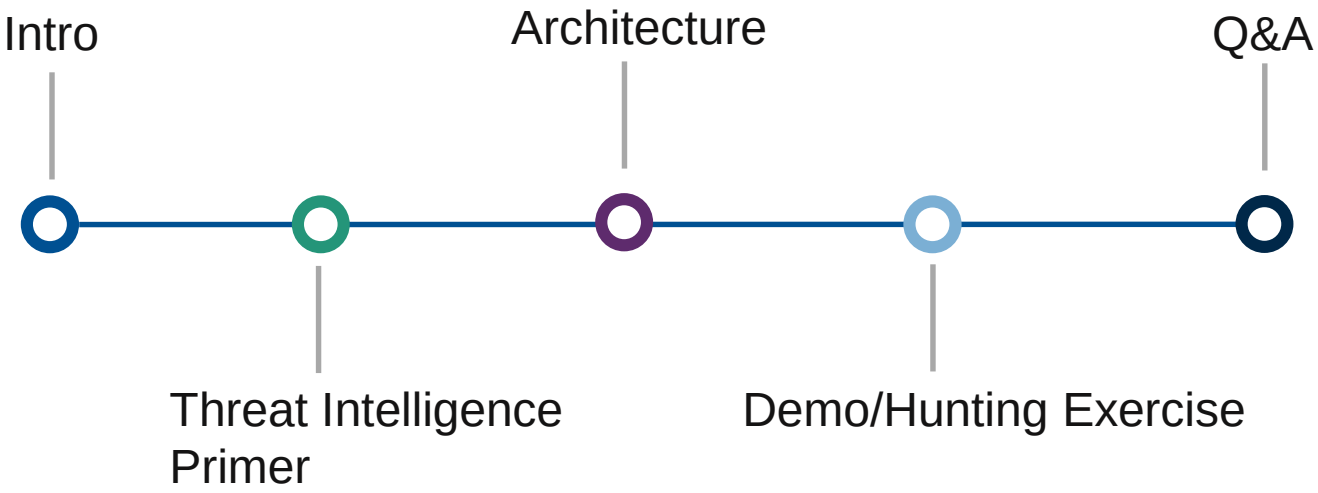
Optiv Threat Intel App for Splunk

Derek Arnold

OPTIV

Agenda



About Your Presenter

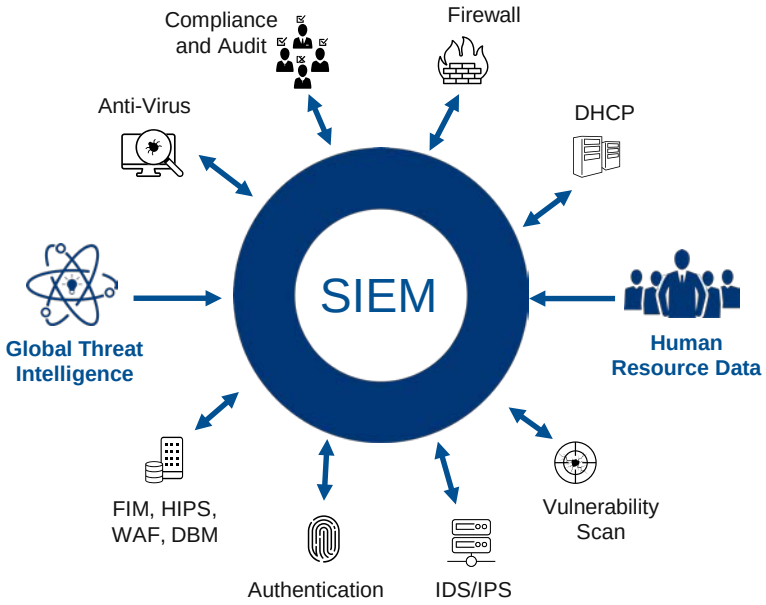
Derek Arnold

- Principal Consultant – Optiv
- 14 years in security
- Focused on enterprise IT
- Avid indoorsman
- Training for marathon
- Three children under nine

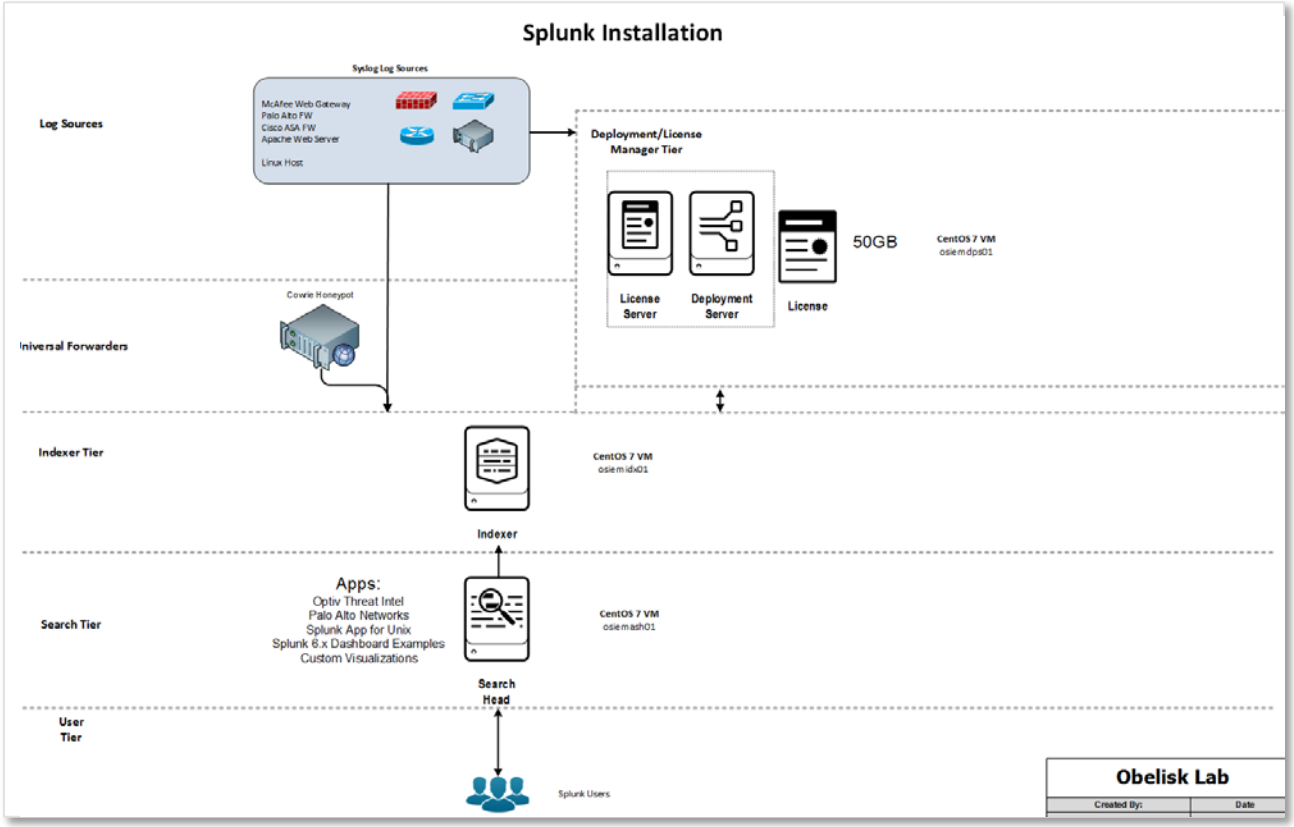
Threat Intelligence Primer

Threat intelligence: *enterprise capability to leverage data, tools and processes together with human assets to approach security in a smarter way.*

- Security Intelligence and Event Management (SIEM) is a key component
- It does not have to be expensive or complicated
- https://www.optiv.com/blog/accessible-threat-intelligence
- https://www.optiv.com/blog/the-business-case-for-an-intelligence-driven-security-program

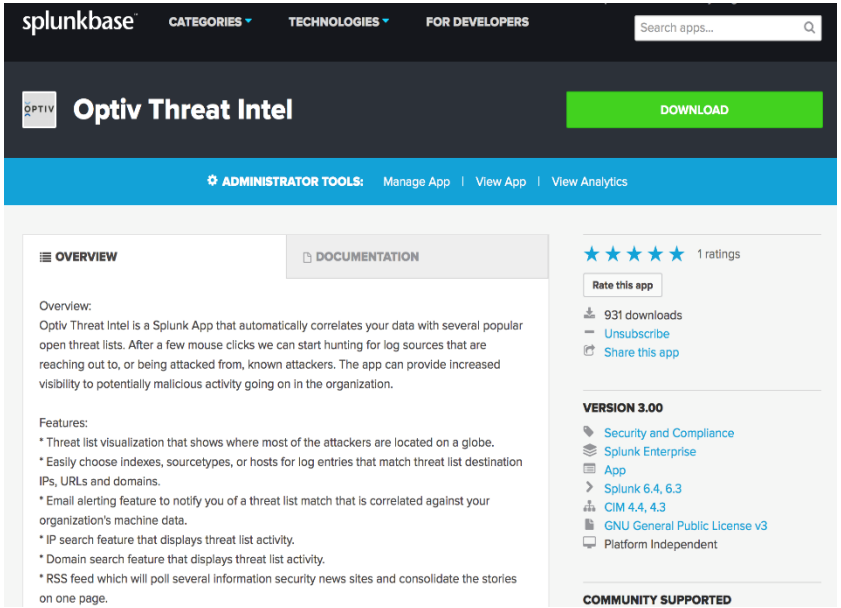


Architecture



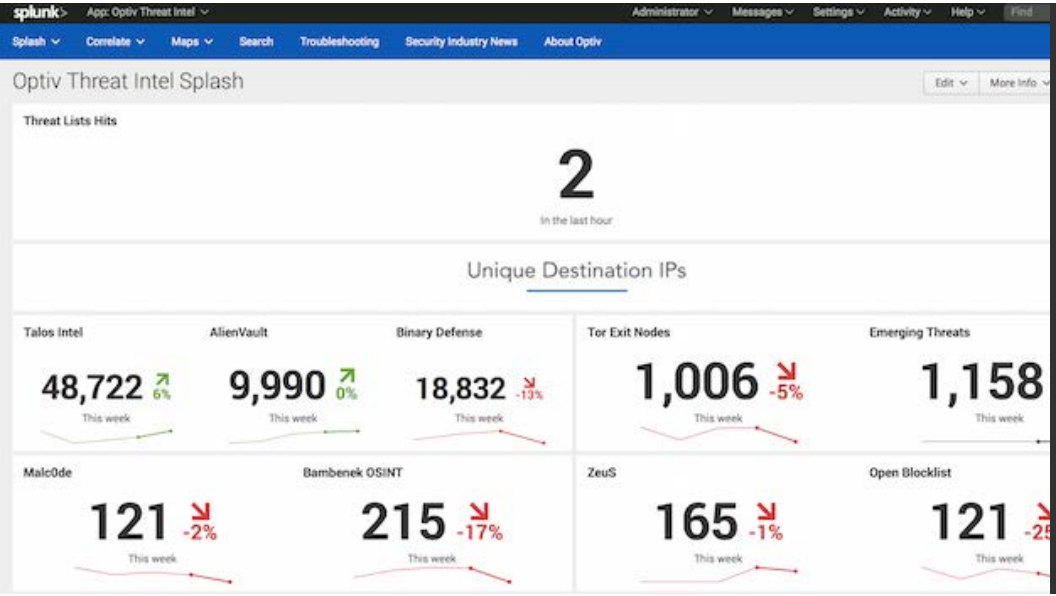
Splunk Apps

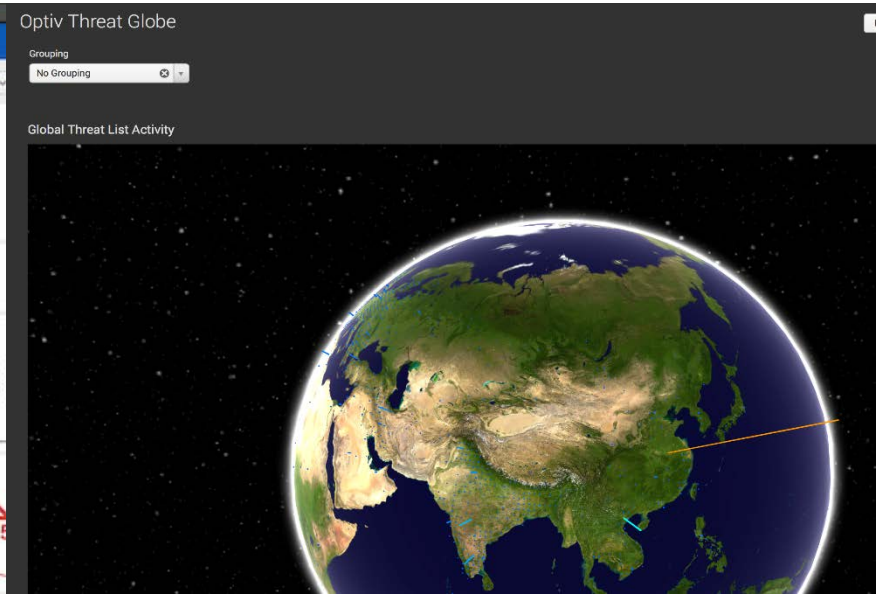
- Splunk can be used as an advanced correlation tool for your machine data
- Other Splunk apps required hardware appliances, premium API keys or advanced configuration
- Nothing was hitting the mark, so I built a new one
- The goal of the app is to provide accessible threat intelligence in a curated setting, with little to no need for configuration or search language knowledge
- In five minutes or less, one can download and install the free app and start collecting and correlating actionable threat intelligence with their organization's machine data
- https://splunkbase.splunk.com/app/2837/



Hunters

Demo / Hunting Exercise





Questions

Derek.Arnold@optiv.com

OPTIV


OPTIV